5G智慧城市安全需求与架构白皮书

IMT-2020(5G)推进组

2020年5月

目录

1 引言 3
2 5G 智慧城市概述 4
2.1 智慧城市 4
2.2 5G 赋能新型智慧城市 4
2.3 5G 智慧城市网络架构 6
3 5G 智慧城市安全需求 7
3.1 终端层安全需求 7
3.2 边缘计算层安全需求 8
3.3 网络层安全需求 9
3.4 行业平台/技术中台层安全需求 10
3.5 应用层安全需求 11
4 5G 智慧城市安全参考架构 12
4.1 5G 智慧城市安全角色 12
4.2 5G 智慧城市安全架构 13
4.3 5G 智慧城市安全技术 14
4.3.1 终端层安全 14
4.3.2 边缘计算层安全 14
4.3.3 网络层安全 15
4.3.4 行业平台/技术中台层安全 18
4.3.5 应用层安全 19
4.3.6 安全运营管理 21
5 5G 智慧城市安全政策和标准 22
5.1 安全政策 22
5.2 安全标准 24
6 5G 智慧城市安全发展建议 26
6.1 加强安全顶层设计和统筹协调 26
6.2 加快安全技术攻关和标准研制 26
6.3 加速安全生态共建和协同发展 26
7 未来展望 27
附录：5G 智慧城市安全应用案例 28
A.1 5G 智慧乌镇 28
A.2 5G 智慧银川 34
A.3 5G 智能厂区 38
A.4 5G 智慧社区 41
致谢 45

1 引言

智慧城市利用信息技术，促进了城市中信息空间、物理空间和社会空间的融合，并通过丰富的应用系统，加速城市经济发展与转型，提高政府及公共服务的效率，方便市民的工作生活，有效地保护和利用环境，实现经济、社会、环境的和谐发展。在当前 5G 等新型基础设施高速发展的背景下，新型智慧城市的建设发展迎来了新的高潮，在 5G、工业互联网、物联网、车联网、大数据中心、人工智能、新能源等新型基础设施的基础上，可进一步推动城市新型管理和服务智慧化，提高城市运行管理和公共服务水平，提升城市居民幸福感和满意度。

5G 给智慧城市发展注入新动能的同时，也带来新的安全风险。而在 5G 智慧城市的不同层面，如终端层、网络层、平台层和应用层等，城市的管理者和建设者都可以部署相应的安全能力来应对这些风险。本白皮书主要分析 5G 技术的应用为智慧城市带来的发展机遇，明确 5G 智慧城市的安全需求，并提出对应的安全参考架构和安全实施建议。

2 5G 智慧城市概述

2.1 智慧城市

根据 ISO（国际标准化组织）的定义，智慧城市指在已建环境中对物理系统、数字系统、人类系统进行有效整合，从而为市民提供一个可持续的、繁荣的、包容性的综合环境系统。2012 年以来，智慧城市成为国际城市化发展的热点之一，全球已启动或在建的智慧城市有 1000 多个，其中在中国超 500 个。传统意义上的智慧城市更加侧重技术层面的问题，其主要内容为构建基础信息网络与云计算平台、配置全方位的感知设备、整合基础信息资源等。新型智慧城市则是在智慧城市发展到一定阶段后更高的一种城市建设发展的形态，更强调新一代信息通信技术与城市现代化的深度融合与迭代演进，进一步提升智慧城市的公共服务效能与政府治理能力，更好地为人民服务，提高城市管理精准化、高效化与透明化。

2.2 5G 赋能新型智慧城市

2020 年 3 月，中共中央政治局常务委员会召开会议提出，加快 5G 网络、数据中心等新型基础设施建设进度。在“新基建”的背景下，新型智慧城市的建设也迎来了新的机遇。新型智慧城市可通过 5G、特高压、城际高速铁路、工业互联网、物联网、车联网、大数据中心、人工智能、新能源等新型基础设施，促进城市中信息空间、物理空间和社会空间的融合，并通过丰富的应用系统，加速城市经济发

展与转型，提高政府及公共服务的效率，方便市民的工作生活，有效地保护和利用环境，实现经济、社会、环境的和谐发展。

5G 高可靠、低时延、大带宽等特性，可高效地将城市的系统和服务打通、集成，提升资源运用的效率，优化城市管理和服务，改善市民生活质量。加快 5G 信息通信技术与城市发展深度融合，通过信息化手段解决城镇化进程中带来的问题，既是城市可持续发展所需，也是产业新动能所在。5G 新型智慧城市具有以下特征:

- 泛在感知。通过全方位的智能感知设备，对城市5G、特高压、城际高速铁路、工业互联网、物联网、车联网、大数据中心、人工智能、新能源等新型基础设施进行数据的实时收集、监控与分析。
- 高效传输。新型智慧城市运用基于5G的高带宽、低时延、低功耗移动信息网络与其他城市信息基础设施实现数据的高效传输。
- 充分融合。智慧城市充分融合5G、特高压、城际高速铁路、工业互联网、物联网、车联网、大数据中心、人工智能、新能源等新型基础设施中的海量数据，提高数据的综合利用与有效管理。
- 协同运作。通过新型智慧城市工业、农业、通信、电力、交通、水利、金融、医疗、公共卫生、社会保障等关键领域运行者与管理者之间的高效协作，实现整个城市资源的优化配置。
- 智能决策。根据新型智慧城市中新基建收集的海量信息，为政府城市治理提供智能化的决策支持，为企业经营和居民的日常生活提供更智能化的服务。
- 精准防控。对城市运行中的突发事件能进行及时预测、预警，能

提供精准的防控，面对突发事件可进行数据、物资、人员的高效配送和协同，城市治理和风险防控能力大大提升。

2.3 5G 智慧城市网络架构

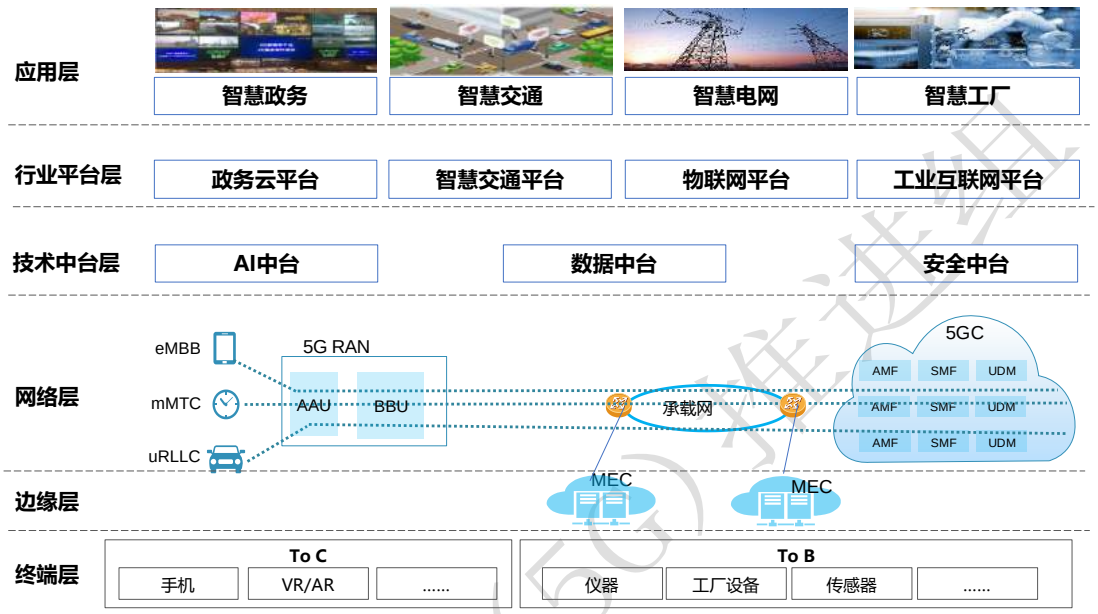

图 1 5G 智慧城市网络架构

5G 智慧城市参考架构包括终端层、边缘层、网络层、数据平台（技术中台层、行业平台层）、应用层，如图 1 所示。其中，终端层主要是面向个人用户的手机终端、VR/AR 终端，以及面向垂直行业的工控终端、CPE（客户前置设备）和各种传感器等。边缘层是 5G 时代面向时延敏感应用的边缘计算云，例如为工业制造、自动驾驶、AR/VR 等应用部署在企业园区或者运营商边缘接入站点的 MEC。网络层是覆盖整个智慧城市的端到端 5G 网络，包括无线基站、承载网、5G 核心网以及 5G 网络切片。技术中台层是一些公共的 IT 中台系统，例如 AI 中台、大数据中台、安全中台等系统。行业平台层是相关垂直行业为了资源、技术的共享复用，集中建设的行业应用平台，例如政务云平

台、智慧交通平台、工业互联网平台。应用层是让城市变得精细、智能和便捷的各种智慧应用系统，包括智慧政务、智慧交通、智能制造、智慧电网等。

3 5G 智慧城市安全需求

3.1 终端层安全需求

在 5G 智慧城市中，主要有两类终端，一类是面向个人用户的终端，例如 5G 手机；另一类是面向行业或者用于城市公用基础设施的终端，例如智慧工厂的 5G 工控终端、各种传感器、以及智慧路灯的 5G 终端等。智慧城市的终端数量大、分布面广，而且软件相对不可控，比较容易被黑客入侵攻陷。

对于智慧城市的各种终端来说，安全需求主要包含两方面的内容。首先，终端自身要在软硬件方面做好安全加固与安全防护，避免外部入侵对终端造成破坏或者信息窃取。而且，各种物联网终端、个人消费终端数量庞大，不法攻击者可能利用终端的软硬件漏洞，入侵之后让终端作为肉鸡发起 DDOS 攻击，给网络和智慧城市的业务带来重大损失。

另一方面，终端作为智慧城市业务的起止端点，对一些重要的敏感业务，需要从源头上确保业务数据的安全，尤其是业务数据的机密性和完整性，防止业务信息被窃听篡改。这要求终端具备对业务数据的加密能力，例如对于政府机构的一些专用终端，需要支持保密通话的功能。

3.2 边缘计算层安全需求

5G 时代，由于工业制造、AR/VR、自动驾驶等时延敏感业务的推广应用，MEC 移动边缘计算云得到大量部署。为了避免物理攻击以及网络攻击的跨网渗透和交叉感染，需要关注 MEC 自身的安全管控以及企业网络与运营商 5G 网络之间的隔离。

对 MEC 自身安全来说，首先要关注 MEC 的物理安全。因为 MEC 一般部署在运营商的接入汇聚站点或者行业客户、企业园区的 IT 机房，位置相对偏远、分散，在门禁准入、物理设施安全等方面，条件可能也不太完善。为了防范对 MEC 站点机房的物理入侵破坏，需要考虑部署一些物理安全方面的防护措施，例如监控摄像头、门禁密码锁等。

除了物理安全，MEC 还需要关注自身网络和系统的安全，尤其是需要防范来自外部网络的入侵给 MEC 站点内的设备系统造成破坏。例如修改 MEC 内网络设备的配置，造成网络中断。例如通过边缘计算 APP 的软件漏洞或者 API 接口调用渠道入侵 MEC 内的网络和 IT 系统，植入木马窃取数据。

另外，对于面向垂直行业客户、部署在企业园区的 MEC 场景来说，客户一般对数据的安全性比较敏感，要求企业数据不能出园区，同时要求企业自身的网络和应用系统免受来自于外部网络系统的攻击破坏（包括来自于运营商网络的攻击渗透）。这方面的安全要求，意味着对面向行业客户的 MEC 来说，需要重点考虑行业客户自身网络系统和运营商网络的安全隔离问题。

3.3 网络层安全需求

覆盖城市各个角落的 5G 网络，是新型智慧城市的基础信息动脉。5G 网络本身的安全，是智慧城市安全的重要前提和保障。从网络本身的组成来说，智慧城市的网络层安全重点要关注 RAN 基站空口、承载网、5GC 以及 5G 切片等几方面的安全。

对于 5G UE 终端到基站之间的空口来说，面临的安全威胁主要有三类。第一类是空口的用户数据窃听篡改，第二类是来自于 UE 的空口 DDOS 攻击，第三类是伪基站或者其它攻击源对空口的恶意干扰。5G 智慧城市基站空口的安全，需要针对这三方面的威胁部署相应的安全防护措施。

无线基站到核心网之间的 IP 承载网和光传输网，可以说是整个 5G 网络的基础骨架。承载网如果被入侵破坏，很可能导致 5G 业务大范围的受损甚至中断。由于 5G 智慧城市的所有业务流量都会经过公共的承载网传输，承载网首先要做好不同业务流量的安全隔离。其次，对一些安全等级高的敏感业务，承载网需要保障业务数据的安全，避免通信数据流量被窃听篡改。另外，考虑到承载网对智慧城市业务运行和社会运转的重要意义，承载网需要保障自身的 HA 高可用性，满足电信级高可靠要求。

作为智慧城市 5G 网络的神经中枢，5GC 核心网的安全是整个 5G 网络安全的重中之重。对于 5GC 核心网来说，重点需要关注自身网络和系统的安全，尤其是防范来自外部网络的入侵给 5GC 数据中心内的

设备系统造成破坏，或者给设备网元植入木马窃取敏感的数据信息。除了防范来自网络外部的直接入侵，5GC 核心网数据中心由于包含多种功能网元，安全方面还需要防范数据中心内部的横向攻击渗透，避免一个网元被攻陷导致整个核心网都受到影响。

5GC 核心网数据中心的业务正常运行对 5G 网络甚至整个智慧城市的安全稳定有着至关重要的影响。除了要通过各种安全手段保障 5GC 的安全，还需要考虑 5GC 自身的 HA 容灾备份，确保在关键网元甚至整个 5GC 数据中心都瘫痪（大规模攻击破坏或者地震火灾等意外事故）的情况下，5GC 核心网能维持业务的连续性。

和之前的 2G、3G、4G 无线通信相比，5G 时代新引入了网络切片技术，通过端到端的网络专用切片承载一些重要的关键业务，例如重点行业客户的业务。从安全性的角度来说，5G 网络切片需要关注两方面的安全，第一是切片间的隔离，一个切片出问题不能影响到其它切片；其次是切片的安全接入和安全使用，避免切片资源被越权滥用。

3.4 行业平台/技术中台层安全需求

为了资源、技术的共享复用，在智慧城市的建设中，可以规划部署面向各个垂直行业的行业应用平台，例如政务云平台、警务云平台、智慧交通平台和工业互联网平台，以及面向一些重点 IT 技术的技术中台，例如 AI 中台、数据中台以及安全中台。这些应用平台和技术中台系统涉及到大量数据的加工处理和存储，其中可能包含一些行业机密数据或者用户隐私数据。所以在安全方面首先要关注数据的安

全，确保数据不被泄露篡改，保障数据的机密性、完整性和可用性。

其次，需要关注应用平台和技术中台系统自身的安全，防止通过网络或者 API 接口调用等渠道入侵应用平台和技术中台系统。

另外，考虑到应用平台和技术中台面向整个智慧城市提供基础的服务能力，为了避免由于系统中断给智慧城市的业务带来重大影响，还需要考虑应用平台和技术中台的 HA 高可用问题，确保在系统故障或者瘫痪情况下能通过备份系统继续对外提供服务。

3.5 应用层安全需求

应用层是智慧城市对行业和社会公众提供各种业务应用的软件系统，例如智慧政务系统、交通智能调度、远程医疗、工业智造等。应用层的安全直接关系到智慧城市的各项业务能否正常开展，关系到智慧城市的社会面能否顺利运转。

对于智慧城市来说，有些应用系统既面向内部的管理运维人员，也直接面向企事业单位和社会公众，例如智慧政务系统。这种受众面宽泛的应用系统，涉及的用户账号数量庞大，类别复杂。为了避免非法访问越权访问，保障应用系统的安全，首先需要关注应用账号的身份管理和访问控制。

智慧城市的应用软件系统涉及到行业应用数据的加工处理和存储，也涉及一些用户身份相关的个人隐私数据。所以在安全方面还要关注数据的安全，确保数据不被泄露篡改，保障数据的机密性、完整性和可用性。

对智慧城市的各种业务应用来说，为了避免出现类似于电话短信诈骗等业务滥用，还需要关注业务层面的安全，监测防范利用应用系统平台实施诈骗、窃取、破坏等不法行为。

另外，智慧城市的应用系统直接面向广大行业与社会公众，软件的任何缺陷漏洞都可能被利用，导致应用系统被入侵破坏或者窃取数据。所以，做好应用软件的安全加固是智慧城市应用层安全的重要工作。

4 5G 智慧城市安全参考架构

4.1 5G 智慧城市安全角色

4.1.1智慧城市安全管理者

智慧城市安全管理者的职责包括但不限于：制定智慧城市安全总体方针、规划、框架，建立智慧城市安全管理组织架构和机制，统筹协调智慧城市安全管理与监督工作，检查、评估智慧城市安全建设与运营工作，定期审核、改进智慧城市安全管理制度和流程，为智慧城市安全的其他角色提供指导和必要支持。

4.1.2智慧城市安全运营者

智慧城市安全运营者的职责包括但不限于：负责智慧城市安全建设、运行与维护管理，部署有效的智慧城市安全防护措施，检测智慧城市安全风险，分析智慧城市安全态势，发现智慧城市安全事件和脆弱性，防范、阻断网络攻击，并负责智慧城市安全风险与安全事件的应急处置和管理。

4.1.3智慧城市安全服务提供者

智慧城市安全服务提供者的职责包括但不限于：设计开发安全产品与应用并提供维护技术服务，为智慧城市安全运行提供信息安全基础服务，部署安全技术措施，协助智慧城市安全运行者进行安全工程建设、运维及应急处置和管理，提供安全产品、服务及技术服务支持。

4.1.4智慧城市安全服务使用者

智慧城市安全服务使用者的职责包括但不限于：合理使用智慧城市服务提供者提供的智慧应用和服务并反馈合理的安全需求，负责所拥有信息数据资产和智慧城市业务的安全管理，定期安排对网络、信息系统和设备进行安全评估，根据评估结果进行整改和修复。

4.2 5G 智慧城市安全架构

GB/T 37971-2019《信息安全技术 智慧城市安全体系框架》提出了智慧城市安全体系框架。参考该架构，结合 5G 智慧城市架构，提出 5G 智慧城市安全参考框架，如图 2 所示。

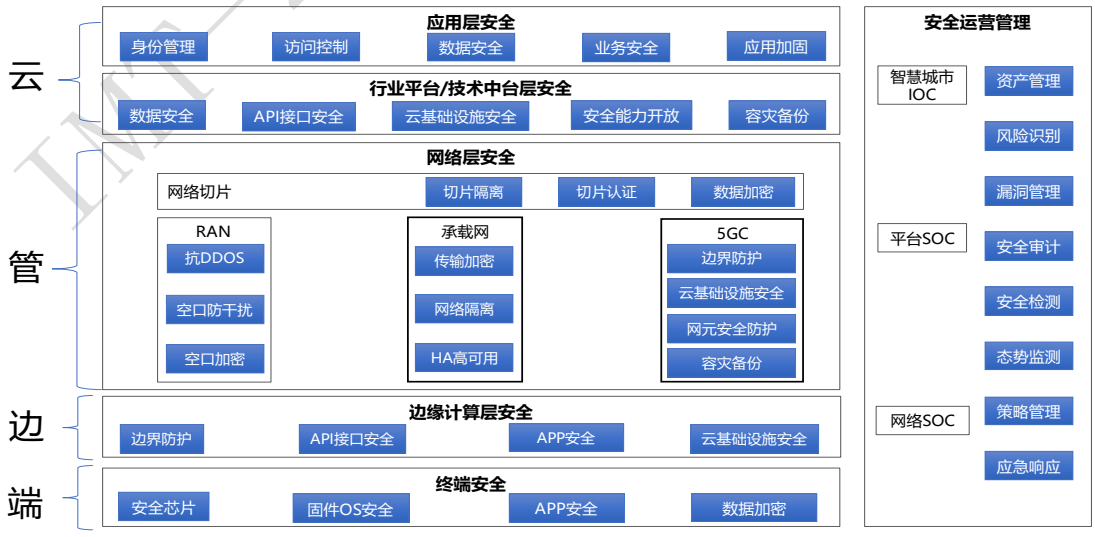

图 2 5G 智慧城市安全体系框架

图中，包括终端安全、边缘计算层安全、网络层安全、行业平台/技术中台层安全、应用层安全，以及跨各层的安全运营管理。

4.3 5G 智慧城市安全技术

4.3.1终端层安全

对于终端来说，主要从底层软硬件和上层应用 APP/数据两个方面保障通信安全。例如，终端内置特殊的安全芯片，作为终端标识、通信加密秘钥和安全可信根的载体，另外通过调试接口物理关闭、物理写保护等措施防范针对终端的底层物理攻击。同时，通过安全启动、完整性校验等措施确保终端的系统固件和操作系统安全。

为了保障终端通信业务的安全，可以对通信数据进行端到端的加密（例如保密通话），防止终端的通信数据被窃听或篡改，避免因为通信数据内容的泄密篡改对智慧城市的业务应用带来破坏或者重大的安全事故。另外，对终端的应用 APP 软件实施漏洞扫描、安全加固等措施，避免因为应用软件的漏洞导致终端被入侵破坏。

4.3.2边缘计算层安全

对于 MEC 安全来说，除了站点物理层面的安保设施，例如监控摄像头、门禁密码锁，首先要做好 MEC 软硬件系统的边界防护，在 UPF 设备的对外接口处（例如连接 Internet 的 N6 接口）部署防火墙等边界隔离防护措施，避免来自于外部网络对 MEC 的入侵和破坏。

确保 MEC 云基础设施的安全是 MEC 自身安全的重要组成部分，例

如通过 VDC、VPC 资源隔离，Hypervisor 安全监控（防虚机逃逸），操作系统数据库漏洞扫描、安全加固等方面的措施，保障 MEC 云基础设施的安全。

另外，在 MEC 边缘计算云的部署应用中，可能涉及到各种应用 APP，以及业务能力 API 的开放对接。需要通过安全扫描加固等措施保障应用 APP 的安全，避免因为 APP 的安全漏洞隐患给整个 MEC 带来损失破坏。同时，可以通过 API 通信接口加密（例如 TLS 加密）和接口安全认证等措施保障 API 接口调用的安全，避免通过 API 对接的渠道入侵破坏应用 APP 以及整个 MEC。

对于面向垂直行业客户、部署在企业园区的 MEC 场景来说，可以在 MEC 和企业网络的边界处（尤其是企业网络侧）部署防火墙、入侵检测系统和网络流量探针等安全设施，一方面确保企业内部信息系统和外部网络之间的安全隔离，另外一方面通过隔离和流量监控等手段，确保企业数据不出园区。

4.3.3网络层安全

从网络本身的组成来说，智慧城市的网络层安全主要包含 RAN 基站空口安全、承载网安全、5GC 安全以及 5G 切片安全等几个部分:

◆ 基站空口侧安全

对于 5G UE 终端到基站之间的空口来说，面临的安全威胁主要有三类。第一类是空口的用户数据窃听篡改，为了应对此安全威胁，可以开启 SUCI 加密以及空口 PDCP 层面数据包的加密功能。第二类是来

自于 UE 的空口 DDOS 攻击，为了防范这种攻击，可以部署 DDOS 检测防御系统，在出现 DDOS 大流量攻击的时候，基站可以做一些限流控制。第三类是伪基站或者其它攻击源对空口的恶意干扰，例如通过伪基站发送垃圾短信、通过特殊信号源实施频谱干扰。为此可以在全网部署统一的伪基站检测系统和频谱干扰检测系统，做到第一时间发现定位网络中的空口干扰源。

◆ 承载网安全

对于承载网的安全，主要从以下几方面来考虑实施。在网络本身的规划设计上，做好 HA 高可用设计，避免单点故障，例如承载网双平面保护倒换。其次，可以考虑部署 IPSEC 安全加密，保障网络数据报文的机密性和完整性，避免业务流量非法监听或者网络重放攻击。

在承载网的协议控制面上，可以配置 MD5 认证或者 SSL 加密等安全措施，避免可能的路由协议攻击（例如 BGP 路由劫持攻击）。另外，通过 VLAN、FlexE、VPN 等技术措施实施承载网的逻辑或物理隔离，不同业务或者不同运营商的 5G 流量通过相互间隔离的管道来承载。

◆ 5GC 核心网安全

对于 5GC 核心网来说，需要从四个方面考虑核心网业务的安全保障措施，分别是 5GC 电信云数据中心的边界安全、电信云 I 层云化基础设施的安全、5GC 网元自身的安全以及 5GC 电信云数据中心的容灾备份。

为了避免来自外部的入侵对 5GC 核心网造成破坏，可以在 5GC 电信云数据中心出口边界处，集中部署防火墙、沙箱、WAF、IPS、抗

DDOS 等安全设施，防御从数据中心外部过来的各种可能的安全威胁。

5G 核心网的一个重要特征是功能网元的虚拟化云化，数据中心云化基础设施的安全是 5GC 安全的重要基础和前提。可以通过 VDC、VPC 资源隔离，Hypervisor 安全监控（防虚机逃逸），操作系统数据库漏洞扫描、安全加固等方面的措施，保障 5GC 云基础设施的安全。

5GC 安全的主要目标是确保 5G 核心网网元的安全稳定运行，除了周边及配套系统的安全措施，核心网网元自身也可以部署一些安全功能来保障网元的安全。例如，在网元系统上安装运行内生的安全组件，监控网元的运行状况，防范可能的病毒木马。同时，还可以通过白名单 ACL、网络微分段、关闭不使用的端口等最小化安全手段对核心网网元的通信进行细粒度的隔离防护，减少网元的安全暴露面，规避安全风险。

另外，对于 5GC 建议规划和部署异地灾备数据中心，确保在遇到火灾、地震或者大规模入侵破坏安全事故的情况下，5G 核心网的业务能在第一时间恢复，保障 5G 网络业务的连续性，减少灾难带来的损失。

◆ 5G 切片安全

对 5G 网络切片安全来说，首先要确保切片间的隔离，一个切片出问题不能影响到其它切片。切片隔离可以分为物理隔离和逻辑隔离，对安全等级和资源保障要求高的重点行业应用，可以部署物理隔离，例如在核心网侧不同切片部署在不同物理服务器上。对于安全性要求不是太高的非敏感业务，可以采用切片逻辑隔离，例如核心网的虚机

隔离。

另一方面，切片安全需保证切片的安全接入和安全使用，例如只有通过切片使用者（政府机构，工矿企业）以及 5G 网络运营商的双重认证和授权，才能接入到对应的网络切片，确保切片的合法接入以及切片资源的合法使用。另外，还可以通过端到端的数据加密，保障切片业务的机密性和完整性。

4.3.4行业平台/技术中台层安全

对于行业平台和技术中台的安全稳定运行来说，主要保障措施体现在数据安全、通信接口安全、云基础设施的安全以及平台系统的容灾备份等方面。

为了避免行业应用平台和 IT 中台的数据被泄露篡改，保障数据的机密性、完整性和可用性，可以部署一些数据安全方面的措施，例如数据加密存储、数据匿名化处理、数据安全删除以及数据的定期备份等。

行业平台/技术中台层的通信接口安全，主要是平台/中台系统与上下游相关的其它部件系统或者网元之间的各种 API 调用、信息采集传递、操作指令传送的安全。这方面的安全保障措施主要有通信接口加密（例如 TLS 加密）、接口认证等方面，避免攻击者通过机机间的通信接口入侵和窃取敏感数据。

在云计算技术日益普及的今天，智慧城市的行业平台和技术中台系统一般也是虚拟化部署，构建在以通用服务器为核心的云化基础设

施之上。为此，需要部署相应的一些安全措施，保障云基础设施底座的安全，例如资源隔离、操作系统数据库安全扫描加固、Hypervisor 安全监控等。

对于智慧城市的行业平台/技术中台来说，为了避免在遇到突发事故灾害情况下系统中断给智慧城市各行各业带来损失和破坏，建议对关键的行业平台和技术中台规划部署容灾备份系统，一些对国计民生、社会稳定有重要影响的系统甚至可以考虑异地灾备。

另外，对广大行业客户这样的智慧城市服务使用者来说，能购买、享受的服务除了智能便捷的信息管道和应用系统，还包括与信息系统配套的安全服务，毕竟，安全是业务正常开展的重要前提和保障。对不同行业领域的各个企事业单位来说，所需要的信息安全功能可能是类似甚至相同的。在智慧城市安全的建设和运营管理中，可以规划建设公共的安全中台。通过这个安全能力服务平台，使能智慧城市的垂直行业应用，将一些常用的安全能力（例如防火墙隔离保护，数据加密，云基础设施安全）通过 API 的形式开放给上层业务系统和各个垂直行业客户，既满足了智慧城市各领域的安全需求，又实现了资源的集约高效利用。

4.3.5应用层安全

对于智慧城市的应用层安全来说，需要关注应用账号的身份和访问控制、数据安全、业务安全以及应用软件的安全加固等方面。

通常每个应用系统会配置多个不同类别、不同权限等级的用户账

号。尤其对智慧城市的一些应用来说，同时面向行业与广大社会公众提供服务，为了避免非法访问越权访问，保障应用系统的安全，需要对应用系统实施严格的身份管理和访问控制，清晰地定义每个用户的角色（例如系统管理员，普通外部用户）、认证方式（例如双因素认证，生物特征认证）和访问权限，做到基于角色的访问控制（不同级别账号可用可见的操作命令和功能菜单不一样）。另外，在用户账号和身份数据的添加、修改、删除上，进行严格规范的管理，同时对账号的访问操作实施例行的监管和审计。

智慧城市的应用软件系统可能涉及行业数据和用户隐私数据的处理，为了确保数据不被泄露篡改，保障行业和用户敏感数据的机密性、完整性和可用性，需要部署一些数据安全方面的措施，例如数据加密存储、数据匿名化处理、数据安全删除以及数据的定期备份等。

对智慧城市的应用层安全来说，还需要防止业务本身被恶意滥用。这方面可以借鉴电信运营商和公安系统防范治理电信诈骗的一些思路，通过基于 AI、大数据等先进技术的行为分析、流量分析和过滤筛查等手段，监测防范利用智慧城市业务实施的各种诈骗、窃取等不法行为。

另外，为了避免软件的缺陷漏洞被恶意利用，还需要通过应用软件系统定期的漏洞扫描和安全加固措施，保障智慧城市应用层的业务安全。

4.3.6安全运营管理

安全三分靠技术，七分靠管理。对于智慧城市运行的安全保障来说，技术再先进，手段再完备，如果在运营管理层面没有严格的落实执行，也很难起到安全保障应有的效果。另外一方面，周密完善的安全运营管理和安全监控响应，本身也是安全保障的重要手段。

在信息系统安全保障工作中，一般会通过安全运营中心（SOC）的组织管理形式统一落实安全的管理、监控、响应、恢复、审计等措施。对 5G 智慧城市的安全保障体系来说，在城市全局层面可以规划建设智能运营中心（IOC）。一方面，IOC 面向业务和社会运转落地实施智慧城市的运营管理，另外一方面，IOC 也面向安全保障承接智慧城市 SOC 的职责。通过 IOC，智慧城市的管理者和运营者能够实时感知整个城市的安全态势状况，对安全事件及时做出全局性的响应和处置。

除了面向城市全局的 IOC，还可以面向智慧城市的各个行业平台，规划建设平台的 SOC。平台 SOC 由行业自身建设运营，例如，城市政府建设运营政务云平台的 SOC，交通管理部门建设运营智慧交通平台的 SOC。通过平台 SOC 的集中监控运营，保障行业平台以及行业内客户应用的安全。

另外，5G 网络是 5G 智慧城市重要的信息动脉，为了保障 5G 网络的安全稳定运行，移动运营商也可以规划建设面向整个网络的 SOC。

5 5G 智慧城市安全政策和标准

5.1 安全政策

智慧城市的安全发展是国际社会关注的热点问题，目前世界主要国家已颁布相关法规和政策文件来推动智慧城市的安全建设。

国际上，美国、欧盟、英国、新加坡等国家与地区都在推动智慧城市部署建设相关政策制度，在升级发展的同时强化安全。总体来看，多数国家由政府部门统筹智慧城市发展与安全，部分国家较为关注信息和数据安全，但普遍缺乏应对智慧城市网络安全威胁的专门政策。主要国家具体情况如下：美国重点关注智慧城市带来的安全和隐私问题，2015 年发布《白宫智慧城市行动倡议》，指出在智慧城市建设过程中要充分利用联邦政府在网络安全等方面已经开展的工作，认为以往在网络安全方面的研究和投资已为智慧城市建设奠定坚实基础，纽约市政府公布了“智慧城市实施方案”，统筹智慧城市发展与安全；欧盟提出“智慧城市与社区欧洲创新伙伴行动”，由牵头政府部门主导智慧城市的发展和安全，倡导在 ICT 技术支持下建设可持续、安全互通的综合交通和物流运输系统；英国在智慧城市建设中重点关注信息安全，2013 年发布《智慧伦敦计划》，提出数据开放等七大发展方向，另外，伦敦政府联合其他机构建立安全机构，为公共机构、企业等应对智慧城市网络威胁提供建议和保护；新加坡政府在智慧城市建设中强化重要数据的保护，提出了“智慧国 2025”计划，由政府统筹构建“智慧国平台”，通过全国数据的连接、收集和分析，提供优

质的公共服务。在这一过程中，新加坡政府重视重要数据的保护，对比较重要的传感器数据进行匿名化保护和管理，并只在一定程度上进行适当的分享。

2014 年 8 月 27 日，国家发展改革委、工业和信息化部等八部委联合印发了《关于促进智慧城市健康发展的指导意见》，这是我国首部全面系统提升智慧城市安全的政策，确定了智慧城市建设“可管可控，确保安全”的基本原则，提出要落实国家信息安全等级保护制度，强化网络和信息安全管理，落实责任机制，健全网络和信息安全标准体系，加大依法管理网络和保护个人信息的力度，加强要害信息系统和信息基础设施安全保障，确保安全可控。《指导意见》提出了“网络安全长效化”的主要目标，建立城市网络安全保障体系和管理制度；明确了“城市人民政府”作为责任主体的网络安全责任制，严格全流程网络安全管理，在重要信息系统设计阶段、实施阶段、运行阶段均提出了相应的要求。2015 年 8 月 26 日，公安部会同中央网信办、国家发改委、工信部共同制定出台了《关于加强智慧城市网络安全管理工作的若干意见》，以促进智慧城市建设安全、健康、有序发展。2018 年 1 月 7 日，中办、国办印发了《关于推进城市安全发展的意见》，以积极推广先进安全技术、提高安全监测和防控能力。

上述一系列规范性文件实施后，我国逐步形成了各部门联合制定、实施智慧城市安全政策的联合监管机制。与此同时，地方相关政策和安全环境逐步完善，各地先后出台智慧城市相关意见，助力智慧城市安全建设。例如，2018 年 7 月 18 日，深圳市人民政策办公厅印

发《深圳市新型智慧城市建设总体方案》，为保障网络空间安全运行和信息安全，提出了“机制保障安全”和“五位一体体系”；2020 年 2 月 10 日，上海市政府出台《关于进一步加快智慧城市建设的若干意见》，提出要“切实保障网络空间安全”，率先推行首席网络安全官制度、提升信息安全事件响应速度、完善公共数据和个人信息保护、加大网络有害信息治理力度等举措。另外，银川市出台了智慧城市地方性法规，明确指出智慧城市大数据主管部门会同有关部门制定数据安全等级保护、风险测评、应急防范等安全制度，加强对大数据安全技术、设备和服务提供商的风险评估和安全管理，建立健全大数据安全保障和安全评估体系；天津市智慧城市建设“十三五”规划中提出要着力推进信息安全设施升级，建立健全信息安全防护体系，强化网络空间内容监管力度。

目前智慧城市安全领域相关的法律法规制度和政策等方面尚不健全，需要进一步明确和完善智慧城市网络和信息安全的制度和政策，推动智慧城市信息安全和网络安全建设。

5.2 安全标准

目前，智慧城市安全国际标准化工作主要涉及国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU-T）等。2016 年，ITU-T FG SCC（智慧可持续城市焦点组）在智慧城市安全方面发布了研究报告《智慧可持续城市网际安全、数据保护和弹性》，提出了智慧可持续城市中安全管理、用户认证、关键基础设施保护以及隐

私保护等方面的安全保障建议。2019 年，ISO 发布了首个智慧城市 ICT 领域国际标准：信息技术—智慧城市 ICT 评价指标（ISO/IEC 30146:2019）。该标准从智慧城市 ICT 视角提出了一套适用于全球的综合性评估评价指标，其中信息安全为七大类评价指标之一。2020 年 3 月，国际电信联盟 ITU-T SG17 工作组通过了我国相关单位提交的《智慧城市数字孪生系统安全机制》和《智慧社区安全机制》两个立项。

智慧城市安全国家标准相关工作主要在全国信息安全标准化技术委员会（TC260）开展。目前发布了 GB/T 37971-2019《信息安全技术 智慧城市安全体系框架》国家标准，并开展了《信息安全技术 智慧城市建设信息安全保障指南》、《信息安全技术 智慧城市网络安全评价方法》、《信息安全技术 智慧城市公共支撑与服务平台安全要求》等国家标准研制项目。

国内与智慧城市相关的行业标准化组织包括：信息、通信、城市、建筑及居住区、运输、地理、商业、信息安全、物流、轨道交通、减灾救灾、食品安全、遥感、电力等多个领域。其中，通信领域行业标准主要在中国通信标准化协会中国通信标准化协会（CCSA）泛在网技术工作委员会研究制定，重点开展智慧城市术语、总体架构、评估方法及指标体系等相关标准研究。目前已发布 YD/T 3473-2019《智慧城市 敏感信息定义及分类》等行业标准。

6 5G 智慧城市安全发展建议

6.1 加强安全顶层设计和统筹协调

建议从国家和地方政府层面加强 5G 智慧城市应用和产业发展方面的安全顶层设计，坚持发展与安全并重、鼓励与规范并举的理念，建设 5G 智慧城市安全应用示范区和创新中心，通过典型试点示范形式，引领更多行业参与 5G 新型智慧城市建设，持续开展 5G 智慧城市安全能力建设；同时，推动跨部门、跨领域间的协作，打通行业壁垒、畅通合作渠道、形成支持合力，协作推动 5G 新型智慧城市的安全发展。

6.2 加快安全技术攻关和标准研制

智慧城市通过跨部门、跨系统的信息交互，实现行业系统之间信息共享和业务协同，各环节均可能存在安全问题。综合国内外智慧城市发展及标准化现状，建议加大智慧城市安全运营、安全态势感知等关键技术攻关，加快 5G 业务应用领域的通用安全标准和重点垂直行业安全指南的研制。

6.3 加速安全生态共建和协同发展

建议建立 5G 新型智慧城市安全合作联盟，团结 5G 设备供应商、网络服务供应商、垂直行业客户、解决方案提供商等产业链各方，围绕 5G 新型智慧城市终端、边缘计算、网络、行业平台/技术中台层、安全运营等方面，协同开展 5G 新型智慧城市跨行业安全应用创新，

建立 5G 新型智慧城市应用的安全生态体系。

7 未来展望

智慧城市是城市智能化、运营可持续化的先进模式，是未来城市发展的必然趋势。5G 网络的大规模连接能力、高速率传输能力是智慧城市建设的有力支撑，实现了对智慧城市的赋能。

为了与智慧城市的网络、业务、数据需求匹配，安全建设应与 5G 智慧城市建设同步规划、同步建设、同步使用。产业各方需重点完善 5G 智慧城市安全标准规范，开展 5G 智慧城市安全应用示范，做好 5G 智慧城市的网络安全保障和平台安全防护，深化 5G 智慧城市应用的安全测评，不断完善 5G 智慧城市网络安全体系。

未来，基于智慧城市的不断发展，5G、人工智能、大数据的能力将不断融合，并最终实现智慧的数字孪生城市。在此过程中，安全框架与安全能力将不断演进与完善，切片安全、安全智能、数据安全、安全可视化等技术将得到深化应用，最终为政府、行业、人民提供更便利、更安全的城市生活环境！

附录：5G 智慧城市安全应用案例

A.1 5G 智慧乌镇

1、应用简介

中国移动在乌镇建设了 5G 未来城镇运营中心，以城市管理、社会管理和应急管理的业务需求为导向，以实战应用为核心，利用 5G 相关能力，实现对城市范围内的体征监测、事件监控、信息报告、综合研判、可视化指挥调度、紧急救援、移动应急指挥、辅助决策等主要功能；建成“机制领先、信息灵通、研判精确、指挥高效、技术先进”的现代化城市智能运营中心，为城镇提供了安全的智慧应用场景。

图 A.1 乌镇 5G 未来城镇运营中心

乌镇 5G 未来城镇运营中心典型的应用场景包括:

1) 建设运行监测系统，实现城市动态监控

建设城市运行综合检测系统，及时全面的掌握城市的运行态势。城市运营管理中心应实现城市运行信息的全面整合共享和跨部门、跨

区域、跨层级的信息互通和智能分析。城市管理可以对多部门、多单位的各类信息的态势有整理的掌握，从而以最有效的方式进行掌控管理。城市运行综合检测可以智能判断和预测城市运行中异常情况，做到提前预防、主动应对，降低事件对城市运行的影响。

2）建设城市体征体系，实时掌控城市态势

通过对各领域应用系统的城市运营各项数据的采集，将数据统一汇总到城市公共数据中心，运营中心通过公共信息平台共享接口服务，从海量数据中抽取各种的资源数据，依据运营中心的应用逻辑，梳理出与城市日常管理、应急管理相对应的支撑数据。如：城市人口年龄结构、性别比例、新增人数；法人数量、新增法人数量；城市经济情况、GDP；医院位置、数量、床位数量、空闲床位数；学校位置、数量、人数；重要企业事业单位位置、类型；城市环境指数、温度、风力、风向、天气情况；城市事件数量、未处置数量；扶贫人数、分布；景区游客数量等。

3）建设调度指挥体系，协同联动办理事件

建设统一的系统调度指挥体系，实现城市事件的快速响应与协同联动。协同联动系统统一接入预测预警信息和各部委上报的事件信息，以城市日常运行管理调度和重大事件联动指挥为核心，实现跨部门、跨区域事件的统一受理、统一分拨、协同调度、联合指挥、过程监督和考核评价，构建全面覆盖、反应灵敏、协调有序、联动高效的城市运行协同调度指挥系统，全面提升城市协同治理过程中快速响应、分析研判、动态管控、联动处置和事后评估的能力。

4）建设决策分析体系，辅助城市规划治理

城市运营管理中心要充分分析、挖掘、发挥城市运行中海量信息的价值，通过城市动态监控数据、城市体征数据，结合空间大数据分析技术和专业分析模型，为管理者提供决策依据和辅助分析服务，为城市领导者提供城市发展规划的综合智库，以此提升城市运营管理水平。

5）建设数据治理体系，实现数据互联互通

城市运营管理中心集中整合治理、监控管理城市运行中数据资源，并通过实际需求面向社会共享开放，通过政府各部门、各企业、民众各界开发和共享应用，强化社会监督、推进政府透明，促进群体智慧和多方协同的价值塑造，激发市场活力，发挥数据在智慧城市中的战略作用。

6）建设处理考核体系，全链跟踪事件过程

主要对城市管理的日常事件、突发应急事件进行处置的全过程监督跟踪管理和考核。实现投诉、上访、舆情、宜居、安全等相关事件的派遣，跟踪部门的处置情况。当突发应急事件发生时，通过应急指调度指挥系统完成事前预案制定，事发预案快速启动。

7）建设信息管理体系，实现信息统一发布

实现城市运营管理信息智能化发布，为市民提供更加及时准确的生活出行信息，主要包括预警信息，预测信息，告警信息等。同时向上级部门推送日常保送信息，以及重大突发应急事件。

2、安全需求

在乌镇 5G 未来城镇运营中心建设中，在网络安全、系统安全、数据安全等方面都面临着不同的安全风险。在网络安全方面主要包括对网络、服务器的安全及加固，网络特别是 5G 网络的认证、加密、完整性保护等安全问题；在系统安全方面主要包括设备的接入、帐号权限的认证、系统的负载均衡、入侵防护等安全问题；在数据安全方面，乌镇 5G 未来城镇运营中心汇集有大量政府数据，并且和各委办局之间的都有数据传输、数据交换、数据接口，需在 5G 环境下确保数据全生命周期的安全。此外，运营中心与安防机器人、无人船、警用指挥车等设备实时链接，如何保障设备安全接入到 5G 安全可信的网络中，也是一个重大挑战。

3、安全方案

1) 网络安全

- 防火墙

在出口区安装 VPN 防火墙，外网口连接到互联网，DMZ 口连接公众服务器区，内网口连接到核心交换机。

- 漏洞扫描

在现有的漏洞扫描系统上升级，利用该系统对网络进行检查，查找其中是否有可被黑客利用的漏洞，对系统安全状况进行评估、分析，并对发现的问题提出解决建议从而提高网络系统安全性能的过程。

- 边界防护

在城市运营管理中心的边界设立一定的安全防护措施。在平台的物理网络之间，城市运营管理中心的边界防护技术和产品主要采用交

换机和综合安全网关。

- 区域防护

区域防护是一个比边界更小的范围，指在一个区域设立的安全防护措施，具体到城市运营管理中心中，区域是比较小的网段或者网络，城市运营管理中心的区域防护技术和产品采用网络入侵检测系统。

- 节点防护

节点防护是指具体到一台服务器或主机的防护措施，它主要是保护系统的健壮性，消除系统的漏洞。建议城市运营管理中心的节点防护技术和产品采用病毒防范系统、漏洞扫描和网络安全评估分析系统。

2）系统安全

系统安全包括系统运行安全、系统信息安全设计、信任服务体系、权限管理设计，系统的安全性需从各个层次来保证

- 设备接入控制

各接入系统的权限（资源提供、资源需求部门）通过身份认证和用户分配的方法（和 IP 绑定）进行接入控制。

- 服务器负载均衡

负载均衡是建立在城市运营管理中心网络结构之上，用以扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。主要完成以下任务：解决网络拥塞问题，服务就近提供，实现地理位置无关性；为平台提供更好的访问质量；提高服务器响应速度；提高服务器及其他资源的利用效率；避免了网络关键部位出现

单点故障。平台设计中数据库服务器和应用服务器都采用负载均衡和容错设计。

- 权限管理设计

因城市运营管理中心参与角色众多，必须要有完整的权限管理体系对用户进行管理。用户管理集中管理访问系统的用户和权限，管理用户信息包括用户的详细信息、所属的部门和相应权限。内部管理用户权限比较复杂，在权限管理上，系统要支持数据特权、机构权限、客户端权限、流程权限、模块使用特权等全面的权限定义，并且可以根据 IP 地址和时间段控制系统的访问。各种权限可以组合为角色，角色可以嵌套。通过权限管理工具，用户可以方便的进行用户权限配置。

- 身份认证

通过对账号的分级管理功能、用户真实身份鉴别等功能开展身份认证。

- 数据安全加密传输（VPN）

考虑到数据传输的安全性，各接入部门到城市运营管理中心的数据进行 VPN 加密传输。接入部门和平台两端防火墙插卡设备之间运行 IPSecVPN 协议，保证数据在 WIFI、以太网、4G、5G 蜂窝网等网络环境的传输过程中的端到端安全性。

- 数据交换过程的安全保障

平台数据交换过程的安全保障主要指信息在交换过程中不能被非法篡改、不能被非法访问、数据交换后不能抵赖等功能。平台业务

系统在传递消息的过程中可以指定是否采用消息内容的校验，校验方法是由发送消息的业务系统提供消息的原始长度和根据某种约定的验证码生成规则（比如从 MD5 校验规则）生成的验证码。

- 数据交换接口安全设计

平台提供的消息传输接口支持不同的安全标准。对于对安全性要求比较高的业务系统来说，在调用平台的 Restful 接口时使用 HTTPS 协议，保证了传输层面的安全；而对于安全性没那么重要，只想通过很少的改动使用平台功能的业务系统来说，可以通过 HTTP 方式调用平台的 Restful 接口进行消息的传输。

4、实施效果

通过网络安全、系统安全、数据安全全方位的安全体系架构及相关技术，利用防火墙及网络加固为城市运营中心的部署环境提供了安全可靠的网络防护；利用周期性的漏洞扫描、系统的帐号、权限、角色提供可靠的系统应用安全及高可用的负载均衡；利用安全的数据传输协议、交换过程的安全防护及数据接口安全等级定义保障系统在 WIFI、5G 等网络下的可靠传输。通过以上三方面的安全措施对乌镇 5G 未来城镇运营中心的应用进行全方位的安全保障系统。同时通过对系统的实时监控、定期巡检和安全维护作业，持续性的降低系统潜在安全风险，第一时间对安全事件进行响应。

A.2 5G 智慧银川

1、应用简介

银川智慧城市被誉为“中国最具影响力和领先的智慧城市样板点”，创新采用“一图一网一云”技术架构，涵盖平安城市、智慧交通等 10 大系统 13 个单模块，全面覆盖城市管理、便民惠民、产业发展等多个层面，实现统一传感测量、信息共享、数据智能挖掘、实景展示。作为首批建设的智慧城市，在建设规划之初就明确提出信息安全问题是一个十分重要的、可能会影响智慧城市进一步发展的制约因素。因此，银川智慧城市的建设以我国信息安全标准和政策为指导依据，采用行业成熟及最新的安全防护思想和技术，构建高标准、完整的智慧城市信息安全防护体系。

2、安全需求

智慧城市的信息安全风险复杂、多变甚至前所未有。而智慧城市的信息安全体系建设必须以风险需求为导向，既要有技术防护能力，也要有安全管理和安全运维的能力，尤其需要在传统安全防护的基础上大胆改进和创新，方可适应新形势下的安全保障的需要。同时考虑到银川智慧城市业务系统的持续扩展与更新、新技术的应用，整体的安全保障有多方需求。

3、安全方案

银川智慧城市信息安全保障体系参照等级保护三级的标准为指导，以相关安全政策为指导依据，结合银川智慧业务需求及国内外智慧城市发展趋势，从技术防护体系、安全管理体系、安全运维体系三个方面进行保障，打造具备”一个中心，三个能力”的智慧城市信息安全防护体系，为客户提供高标准、合规范的安全保障。

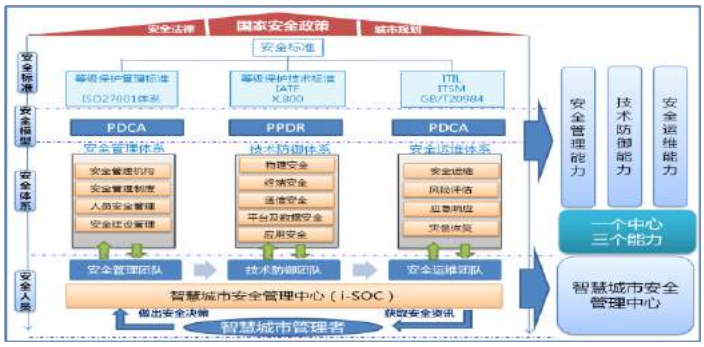

图 A.2 银川智慧城市信息安全体系

安全体系除了遵循物理层、感知层、网络层、数据层和业务层分层结构外，在逻辑的基础网络的规划上分为数据中心、互联网、委办局、传感及专线网络，建设统一的核心交换区来保障接入安全，建设云数据中心来支撑智慧城市的主要智慧业务。因此智慧城市多层安全域实际上是横跨了数据中心、OTN 网及互联网的逻辑结构。其网络结构如下:

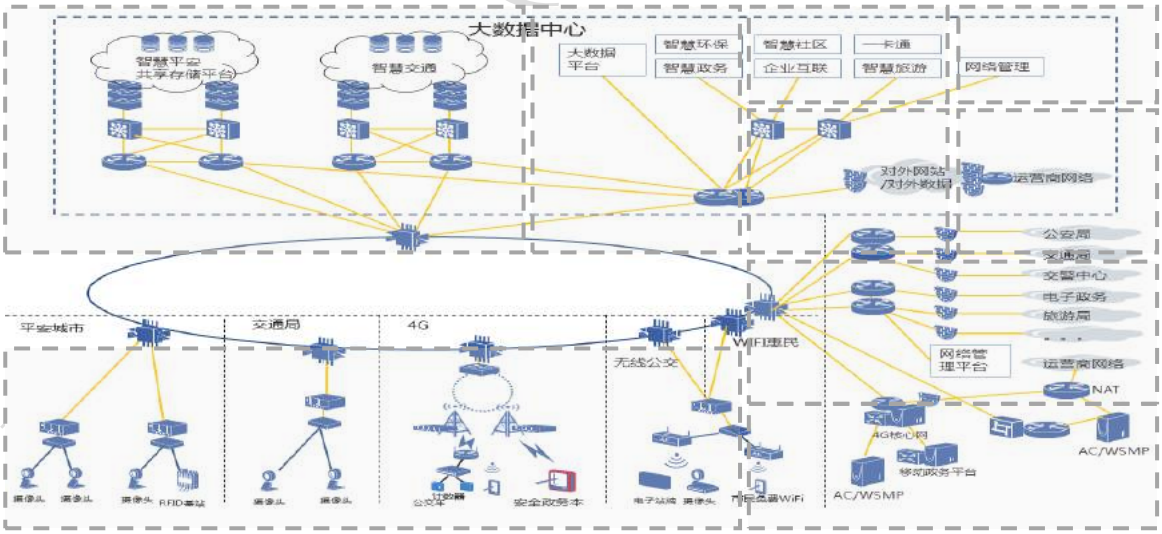

图 A.3 银川智慧城市安全区域逻辑图

整体架构以等级保护的技术要求及深度防御思想为核心的技术防御体系，对银川智慧城市的物理层、感知层、网络层、平台层和应用层提供立体的防护能力。在智慧城市的不同层次采取针对性的安全

防护措施，具体覆盖终端安全、网络传输安全、平台及数据安全、业务应用安全。技术防护体系遵循 PPDR 安全模式，即“策略-保护-检测-反应”，既利用传统的安全设备，如防火墙、IPS 等设备，进行被动检测，又能够利用认证机制、加密机制和风险预测机制来主动防御安全风险。架构创新之处在于，设立统一安全策略中心，对各层安全设备涉及的 ACL 策略、入侵防御策略等进行集中管控。

4、实施效果

银川智慧城市安全方案的实施和推广,构建了智慧银川的信息安全防护体系，信息安全防护体系将传统安全与新安全做全盘考虑，相互结合，在秉承了传统安全标准和防护手段的前提下，还前瞻的结合了移动安全、物联网安全、大数据、云安全等新兴安全的解决思路，所构建的智慧城市的信息安全体系在国家相关政策、法律、城市规划的指导下，参照 ISO27000、等级保护等国内外信息安全标准建设，其核心功能“一个中心，三个能力”总体上具备全面、立体、协同、自主可控的安全特性,安全能力满足等保三级的安全标准。从而为“智慧银川”信息安全保障工作提供了强大的技术支撑能力。

银川智慧城市安全方案的实施使安全运维人员能够及时发现和上报信息安全事件，实施全方位、全时段的安全监控，动态掌握网络安全现状、出现的问题及处理情况。大大提高了网络安全事件的发现率、群众的满意度。

同时，智慧银川的信息安全防护体系还给使用智慧城市业务的企

业、单位和个人提供了健全的信息安全防护能力，有效发现、阻截和追溯网络安全风险及信息安全事件，保障企业、单位和个人的信息不被泄露，有力的支撑了企业办公和个人业务，提升政府、企业及市民的满意度。

A.3 5G 智慧厂区

1、应用简介

智能制造系统主要考虑设备、工装、工具、物料、产品和人员六方面，通过对这六方面的数据采集，及时准确反映生产状态的变化，使设计、工艺、工人能够及时传递工作内容、明确工作任务。采集的数据在网络的承载下，传递给以MES为代表的制造管理系统，为正确应对生产过程中的各种变动提供依据，驱动制造过程按照既定的规则运行。基于对这些数据的加工、处理、分析和提炼，能够改善产品设计、优化生产过程，从而改进生产质量、提高生产效率，为企业创造价值。

充分利用5G具有高带宽、高速度、高可靠、低时延的特点，5G技术在航空智能制造工业园区应用，采集各方面的数据，建立满足制造要求的传输通道，为目前制造提供良好的数据传递。而随着5G等新技术在园区普及应用，且5G目前使用公用频段，使得智能制造系统不但面临实时运行控制系统、特定工业协议和和设备的安全风险，也面临互联网的攻击渗透，将带来更大的网络安全挑战。

图A.4 智慧厂区应用架构图

2、安全需求

针对5G智能制造系统网络安全痛点问题，各层安全需求主要包括:

- 对端设备与访问用户身份认证需求，适配工业现场环境、低功耗模式等重要工业系统端级别的设备实体鉴别需求，以及数字签名实现对操作人员身份的真实性和合法性，提高用户操作的可追溯性。
- 对5G工业网络安全传输需求，适配5G工业网络中不同网络速率和连接数要求的的传输认证和传输加密需求，对重要工业系统的敏感数据进行传输加密，能降低对系统关键数据被窃听及篡改的可能性，确保通信可用和重要工业系统业务正常运行。
- 对数据加密存储需求，重要工业系统中的关键工艺参数、用

户信息等敏感数据信息的安全关乎企业核心竞争力，通过对已有组态系统汇聚数据加密和访问控制，确保数据安全。

3、安全方案

结合等保2.0对工业系统安全扩展要求，对5G智能制造系统安全接入网、安全核心网、安全业务系统、安全应用等主要安全需求，形成基于密码技术的5G智能制造安全防护方案。

以嵌入式安全模块、安全接入网关、服务器密码机、安全认证网关等密码产品为载体，配合安全态势感知等平台支撑，为5G智能制造企业提供全方位的安全保障。

针对终端控制设备，提供支持内嵌式硬件密码模块，实现设备层、边缘层工控协议密码安全，实现海量终端安全接入控制，解决终端身份真实性问题。针对5G公共频段网络提供安全接入网关实现网络传输密码安全保障，解决系统数据传输安全问题；对业务服务器提供调用式服务器密码机，实现业务数据加解密、加密存储等安全应用，解决应用数据机密性、完整性、不可否认性问题；以安全认证网关实现控制系统不同角色用户的身份鉴别和授权访问，解决非法接入问题，达到操作留痕，便于追溯。

4、实施效果

基于安全方案对“5G+工业互联”的飞机制造园区进行试点应用，基于密码技术安全加固方案应用已见成效。5G智能制造安全应用在降低数据失泄风险的同时，可提供智能制造全生产要素与全生命周期安全防护，为工业互联网的落地应用提供坚实的安全保障。

A.4 5G 智慧社区

1、应用简介

该项目位于意大利北部城市 Bergamo 的一个智慧社区项目，占地面积 5 万平方米，集广场、剧院、酒店、住宅、商场于一体，项目的理念是结合现代和著名的建筑与最先进的数字技术，构建一个多代包容的体验平台，为居民和访问者提供绿色、简便、易行的数字化的生活体验。项目采用了微软的智慧应用方案。

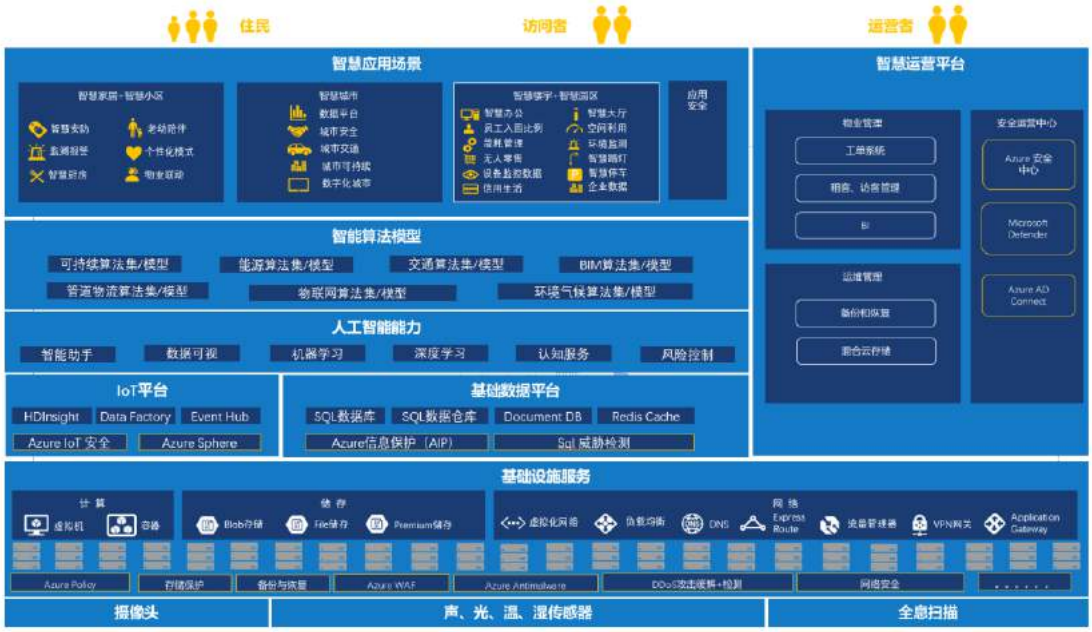

图 A.5 智慧社区应用架构图

智慧社区典型的应用场景包括:

环境管理通过物联网传感器收集相应的环境数据，使用大数据和 AI 技术对数据进行处理和分析，实现了智能化的环境管理和跟踪。

能源管理通过传感器、智能电表搜集用电的数据和信息，结合空间和人的数据，实现智能化能源管理，进而实现能源用量降低。

物业管理采用微软的 dynamics 一体化平台全面支持物业数字化

运营服务。

设备设施管理通过传感器对园区内设备进行全方位监控，使用大数据和人工智能实现预防性维护，提升设备运行效率同时减少维护人力。

安保安防通过实时视频，结合 AI，实现智慧的，低成本的安保安防。

智能社区交互通过利用新一代信息技术来改变企业和公众之间的交互方式，提高交互效率、灵活性和响应速度，实现更加智能运作的园区。

无感通行基于感知层、网络层、平台层、应用层，跟整个大的 IoT 平台做关联，真正实现人行、车行场景的融合，全面迎来无感通行和数字化管理的时代。

2、安全需求

在智慧社区应用中，面临着众多安全风险，其中比较普遍的是管理者对所有授权和未授权的设备/资产缺乏认识，使用缺省的管理员密码，系统中数据加解密弱，缺乏安全性评估和软件代码测试，系统无法对软件和固件进行修补或者更新，易受分布式拒绝服务攻击，居民安全和隐私意识不足，弱口令的使用等，这些风险会导致很多安全问题，比如个人信息泄露，妨碍正常的园区服务，导致财产上的损失，甚至涉及公共健康和人身安全。

此外，在智慧社区中，终端层存在大量的设备和传感器负责提供数据，这些终端中许多使用传统现场总线协议且已经在现场服务多

年，无直接联网能力。同时大量设备基于资源极其匮乏的单片机系统，不具备足够的资源和扩展能力来实现安全所需的特征。因此使用一个安全的数据传输终端将已有的、缺乏安全设计的设备接入到 5G 安全可信的网络中，是保障智慧园区从终端层到平台层端到端安全设计的一个重要挑战。

3、安全方案

案例中用到了微软的 Azure 云作为云端，通过 Azure 内置的安全功能和模块（Azure 活动目录，Azure Policy，Antimalware，DDoS 检测和缓解，存储保护，信息保护，Sql 威胁检测等）在数据保护、基础设施服务安全、平台安全方面发挥了主要作用，同时利用安全的运营中心实现对威胁的检测、安全事件的快速响应和恢复。

IoT 设备端采用 Azure Sphere 解决方案，基于芯片的硬件信任根，并预装为物联网安全定制的 Linux 操作系统，实现了设备的安全可更新、基于硬件的信任根、最小信任基、运行域隔离等防护，通过与其搭配的安全云服务协同，平台层可以完整的验证设备的身份和软件合法性，提供及时的安全系统更新以及收集故障报告以分析潜在威胁。针对既有设备安全联网问题，利用 Azure Sphere Guardian 模块方案，南向通过对接 RS232、RS485、I2C 或者低速无线网络接收传感器模块发送的数据，北向通过 WIFI、以太网、4G、5G 蜂窝网络将数据发送到物联网平台。目前已有多个系统供应商已经实现了可以商业化的蜂窝网络 Guardian 模块。

Azure 在全球获得了 70 多项合规认证，其中包括符合 GB

18030-2005 标准的认证、等级保护三级以及可信云服务认证。

4、实施效果

通过云+边+端一体的可信赖核心技术，利用 Azure 内置的安全功能和模块，以及针对 IoT 平台的保障措施，保障终端安全可信的同时，实现了数据的安全传输，平台和数据的安全防护，对终端、平台软件和固件的及时更新，并能够应对高强度的安全攻击，为应用场景提供了可靠的数据基础和决策的依据，对于实现高效安全的智慧社区应用场景起到了决定性的作用。同时基于 Azure 安全中心的安全运维，使得系统的运维者可以对设备、网络、虚机、数据库等所有资源的安全状态进行持续的监控和分析，获得整个园区的安全态势，提早发现潜在的安全风险，第一时间对安全事件进行响应，对智慧园区的应用进行全方位的安全检测。

致谢

中国移动通信集团有限公司、中国信息通信研究院安全研究所、国家信息中心、华为技术有限公司、中国信息通信科技集团有限公司、中兴通讯股份有限公司、兴唐通信科技有限公司、中国商飞上海飞机制造有限公司